Rendu Cryptographie

Guilhem Marion

Exercice 1

Question 1

Si deux individus ont la même N ainsi que deux clefs publiques/privées differentes c'est qu'ils connaissent $\phi(N)$ [1]. Or,

$$e_1 d_1 = 1(mod\phi(N))$$

et

$$e_2 d_2 = 1(mod\phi(N))$$

Et e_1 et e_2 sont publics et $\phi(N)$ et connu des deux individus, donc on peut retrouver d_1 (respectivement d_1) en calculant l'inverse de la clef publique de l'autre individu modulo $\phi(N)$.

1. Le nombre de nombres entiers en 1 et N.